ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 3, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 6.551

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

Voting Protocol Based on Blockchain with the Highest Levels of Voter Privacy

B.Sundaresan [1],Venati. Sarath [2], M.Guna Sekhar [3], Thota Rajesh [4], Malli.Charan [5]

[(1,2,3,4,5)] Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

ABSTRACT*:* Building a strong electronic voting structure for electronic voting that offers the fairness and security of current democratic plans while providing the straightforwardness and versatility introduced by electronic systems has been difficult for a long time. In this paper in progress, we explore the use of blockchain to help realize the proliferation of electronic democratic structures. The paper proposes an intelligent electronic democracy system considering blockchainthat guards part of the obstacles in existing structures and examines part of the notable blockchain structures for inspiration driving the blockchain-based e-design structure and voting form structure. In particular, we evaluate the development capacity of relevant records through the display of logical examination; expressly a pattern of political raceand implementation of a blockchain-based application that deals with security and reduces the cost of working with political race across countries. We adopt homomorphic encryption and zero-knowledge proof to achieve anonymity and verifiability of encrypted data. Through performance analysis and testing and comparison with existing similar designs, the results show that our scheme has advantages in security and robustness, and the performance test shows that our scheme has good practicality and scalability.

KEYWORDS: BlockChain, e-casting, e-voting, homomorphic encryption, democratic.

I. INTRODUCTION

Elections are crucial to the political process.From the election of the class committee to the election of nationalleaders, voting activities are inseparable. It can be said that voting determines national and local politics. Its importance is self-evident. There have been different ways of voting since ancient times. From the paper ballot in the early days to the electronic ballot commonly used today, the efficiency of voting has increased hundredsof times.

After years of development, the efficiency of the electronic voting system has improved significantly, but its security has not improved much. Paper ballots are still popular in major election campaigns. For example, the 2020 US presidential election was conducted by mail-in paper ballots. During this election, we occasionally saw stories in the news about delays in vote counting or Trump being accused of voter fraud. Regardless of whether these stories are true or not, they indicate that there are still many problems with paper ballots and manual counting. First, the most prominent problem is that the storage of paper ballots takes up a lot of space,and paper ballots cannot be stored for a long time. The second problem is that paper ballots cannot be easily verified by voters, and even if they could, it would take a lot of time and human resources. A third problem isthat paper ballots cannot protect users' privacy well. It is easy to match the real identity of users with the ballots, and the counting process is also prone to errors.

II. LITERATURE REVIEW

Literature research is the most important step in the software development process. Before creating a tool, it is important to determine the time factor, profitability, and strengths of the company. Once these are in place,there are 10 more steps to decide which operating systems and languages you can use to develop your tools. Once programmers start building tools, they need a lot of external support. This support can come from experienced programmers, books, or websites. The above evaluations will be considered in the development of the proposed system before the system is built.

There are several past and ongoing research efforts on the development of electronic voting systems. These works largely focus on requirements, technical specifications, and implementation technologies to support various aspects of elections from registration and verification to voting to count and result. A major shortcoming of these studies is their exclusive focus on the technical aspect of e-voting solutions without significant attention to the human and environmental factors that likely determine the successful adoption of
such e-voting solutions. This paper offers three solutions to this design flaw.First, it provides a conceptual e-voting

system as a socio-technical system [1]. Second, it develops a set of principles to guide the socio- technical design of electronic voting. Thirdly, it offers these ideas' practical applications. The paper concludes with the pragmatics of this approach to e-voting adoption, especially in a setting like Nigeria.

Electronic voting systems promise voters the benefits of accessibility and convenience, allowing themto cast their vote at any time, from any Internet-connected computer device anywhere in the world. However,unlike traditional paper voting systems, the electronic voting system brings several security risks, such as voting privacy, voter disconnection, voter pressure, concealment of partial election results, and verifiability and integrity of voting [6]. Voter authenticity is another security issue, i.e. the voter must be identified through an authentication mechanism that prevents unauthorized voters from voting or multiple votes from authorizedvoters. Another security concern is the handling of votes by an infected (e.g. virus, malware, etc.) voting
device. Since voters use their devices to cast votes in an uncontrolled environment, a malware-hosted devicecould make unauthorized modifications to voter choices. Many electronic voting systems have been proposed, but all of these schemes either do not provide all the required security features or are not practically feasible on lightweight computing devices.

III. METHODOLOGY

We proposed a new method to solve the problem of abstinence in an automatic voting system. Specifically, we first use homomorphic encryption to encrypt the content of the ballot, and then blind the homomorphic encryption result using each voter's secret fragments from sharing the Shamir secret threshold to protect the privacy of the ballot and realize self-counting. at the same time.
Inspired by Camenisch, we designed a new range verification algorithm for our voting system. A new algorithm can ensure that a voter-submitted ballot is well-formed and the voting score is within the legal range. And the content of the ballot will not be disclosed in the verification process.
We implemented the proposed scheme, analyzed its security, and compared the performance. The results showthat our scheme can achieve the predetermined security intensity, the way to deal with abstinence is more practical, and the performance shows that our scheme has good practicality and scalability.
Blockchain is a distributed ledger managed by a decentralized peer-to-peer network. This ledger can only be attached, not deleted. Any changes to the ledger require consensus among all members of the peer-to-peer network. In 2008, Satoshi Nakamoto first proposed the use of blockchain technology as the underlying technology of cryptocurrencies. Blockchain technology has the following important features.

1) Decentralization. The entire network is not controlled by one user or organization. All participants of this blockchain network are equal to the public blockchain, have the right to verify transactions, and participate innetwork consensus.

2) Immutability. The hash of the previous block is contained in the current block. Once transactions are verified and entered into the state database, transactions cannot be withdrawn.

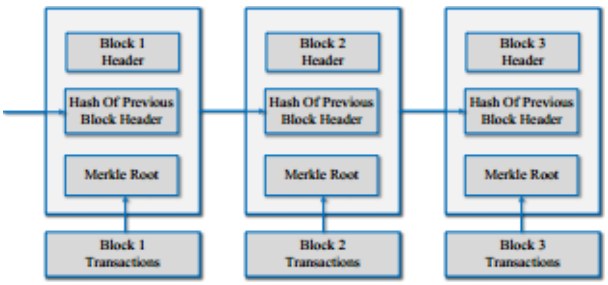


Fig. Block Chain Structure

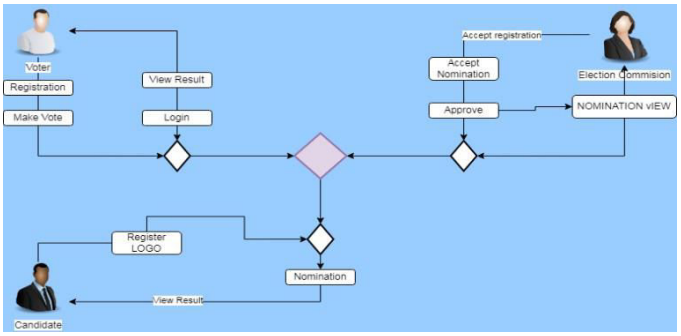
3) Non-repudiation. When a user submits a transaction, a digital signature will be included in it. Anyone canverify the signature using the user's public key. According to the signature characteristic, if a user has signeda transaction with his private key, he cannot say that he did not sign the transaction because no one will believewhat he says.

4) Transparency. Each member of the blockchain has a backup, so we can easily access any data in the blockchain, except the encrypted data associated with the identity.

5) Pseudonymity. Each user will be assigned a blockchain address that is randomly generated and there is no connection between the real identity and the blockchain address. Pseudonymity can be achieved to some extent.

6) Traceability. Blockchain is like a ledger for connections only. All transactions are tracked by the sender of the transaction and the recipient of the transaction.

Smart contracts are code executed on the blockchain. The immutable nature of the blockchain enables the reliable execution of smart contracts with reliable results. Smart contract code can be written, deployed, and run by anyone if we write it according to pre-set rules. The emergence of smart contracts has enabled the widespread adoption of blockchain technology, which is no longer unique to cryptocurrencies. Now blockchain technology can be applied in almost any field such as finance, insurance, supply chain, and so on.



The architecture of the Proposed System

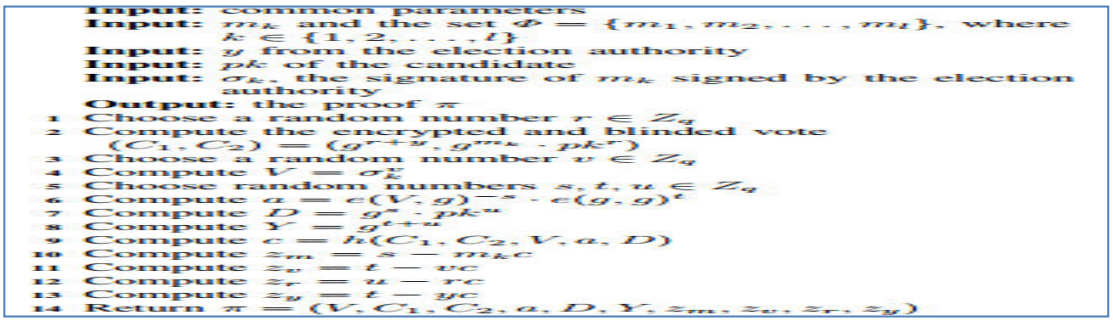
The system architect will determine the basic structure of the system, we will design the Hash code Solomon'salgorithm, and to protect privacy, we can put a small part of the data in the local machine and fog server. Additionally, this approach can determine the percentage of distribution stored on local, cloud, and fog computers using computational intelligence.Through theoretical security analysis and experimental evaluation, the feasibility of our scheme has been verified, which is indeed a strong complement to the existingcloud storage scheme.

ALGORITHM

Camenisch et al. propose a signature-based set membership protocol that can be used to prove that a memberbelongs to a set without revealing any information about it. However, the above proposal cannot be directly used to verify our vote. Because the member we want to prove should be committed by a Pedersen commit, rather than a modified ElGamal ciphertext or a blinded one. In the voting protocol proposed in this paper, the content of the ballot is the ElGamal blind ciphertext, which means that the content of the ballot is cast by theElGamal blind ciphertext. Therefore, the scheme needs to be improved in two stages. The first stage is to design an ElGamal ciphertext extent verification scheme. The second stage is to design a blind ElGamal ciphertext range proof scheme. We have improved the protocol so that it can be applied to our voting protocol. In the first phase, we improved it to make it available to prove that a member encrypted with a modified ElGamal encryption system belongs to a specified set.

Proof Generation Algorithm

Input: common parameters
Input: the proof
$$\pi = (V, C_1, C_2, a, D, Y, z_m, z_v, z_r, z_y)$$
Output: true or false
1 Compute $c = h(C_1, C_2, V, a, D)$
2 Verify if $Y = C_1^c \cdot g^{z_r + z_y}$ holds
3 Verify if $D = C_2^c \cdot pk^{z_r} \cdot g^{z_m}$ holds
4 Verify if $a = e(V, pk)^c \cdot e(V, g)^{-z_m} \cdot e(g, g)^{z_v}$ holds
5 if all verifications pass, return true
6 else return false



Proof Verification Algorithm

IV. RESULTS AND DISCUSSION

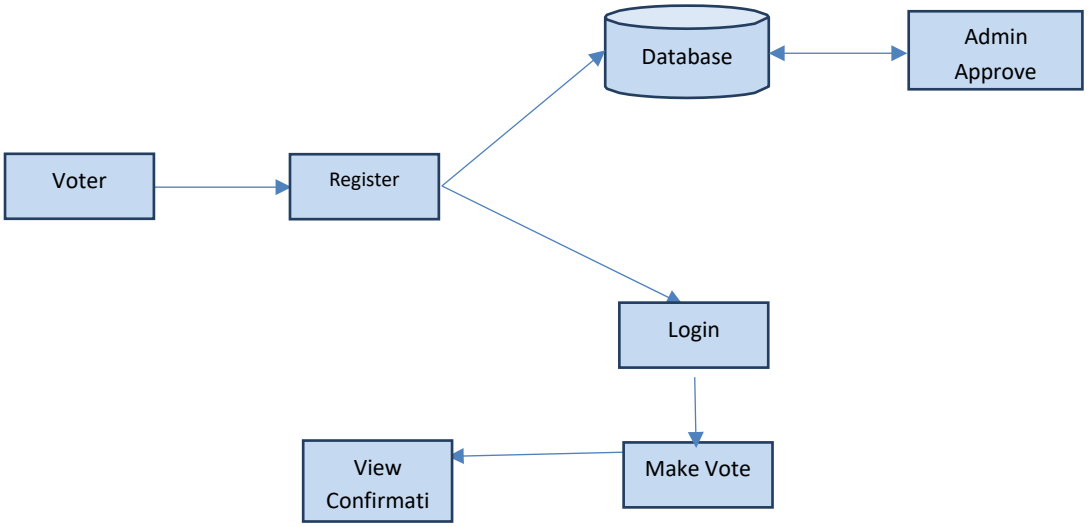
Voter:

I. Apply:
In this module, the voter can request his voting card. When each voter can access the website,they need a unique ID to vote. The voter then applies to the electoral commission.

II. Make vote:
In this module, the voter can vote for candidates. Voters view the list of election candidatesand then select one candidate to vote for.

III. View the vote:
In this module in our project, the voter can view his vote to confirm whether the entered voteis valid or not.

Voter Process Diagram



Election Commission:

i. Approve:

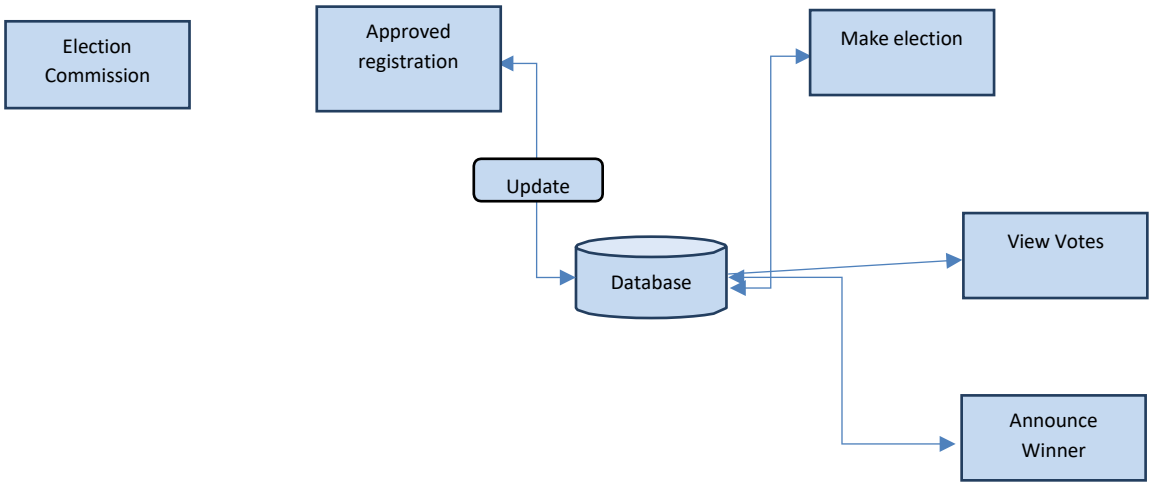
In this module in our project, Election Commission can approve voter registration andcandidate registration after verifying their details.

ii. Election Application:

In this module of our project, the electoral commission reviews the application form of eachcandidate. Approve the nomination after verifying their details.

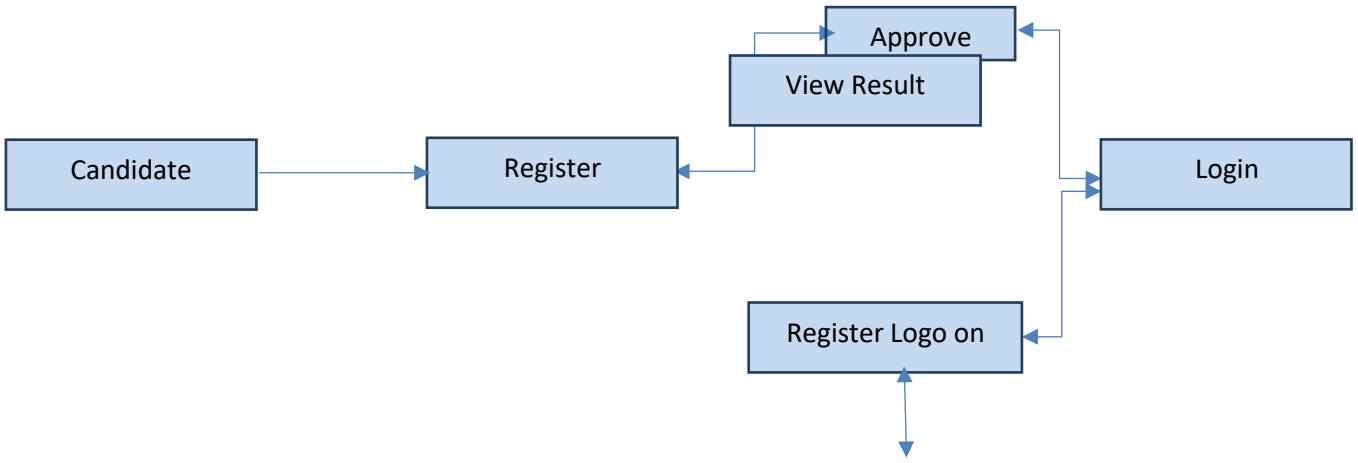
iii. Vote view:

In this module, in our project, the election commission views every vote and the list.



Election commission Process Diagram

Candidate:



Candidate Process Diagram

iv. Nomination:

In this module, in our project, the candidate nominates their details for Election.

v. Approve logo:

In this module, in our project, the candidate needs their nomination identification as name aslogo.

V. CONCLUSION

This web-based voting framework will deal with citizen data through which a voter can log in and exercise their democratic freedoms. The framework will bring together all the important elements of a votingframework. It gives each party the tools to keep up with the citizen vote and has an absolute no. votes of eachparty. There is a data file maintained by the Political Decision COMMISSION in which every voter's name is stored with complete details. We propose a blockchain-based self-voting protocol and an improved proof-of-scaling scheme is proposed to protect vote privacy and prevent malicious voters. This protocol can meet the following security requirements: (1) Voting privacy: the content of the ballot is homomorphically encrypted and calculated on the ciphertext field; (2) Universal verifiability: every participant can verify the validity of ballots and voting results; (3) Robustness: use secret sharing to deal with absences and delays will not changethe protocol process; (4) Freeness: sending blockchain transactions to vote to prevent forced voting and vote buying; (5) Fairness: votes cannot be pre-counted during the voting phase to ensure the fairness of each voter;(6) Self-accounting: Voters calculate the voting results in themselves without the need for a trusted third party.Test results show that the scheme has good applicability to voting scenarios of different scales.

REFERENCES

[1] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Advances in Cryptology — CRYPTO 1992, pages 56–73. Springer, 2004.
[2] Josh Daniel Cohen Benaloh. Verifiable secret ballot elections. Ph.D. thesis, Yale University, 1987. [24] Josh D Cohen and Michael J Fischer. A robust and verifiable cryptographically secure election scheme. Yale University. Department of Computer Science, 1985.
[3] Kazue Sako and Joe Kilian. Receipt-free mix-type voting scheme. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 393–403. Springer, 1995.
[4] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large-scale elections. In International Workshop on Security Protocols, pages 25–35. Springer, 1997.
[5] Martin Hirt and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 539–556. Springer, 2000.
[6] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Advances in Cryptology — CRYPTO' 86, pages 186–194, Berlin, Heidelberg, 1987. Springer Berlin Heidelberg.
[7] Wenlei Qu, Lei Wu, Wei Wang, Zhaoman Liu, and Hao Wang. An electronic voting protocol based on blockchain and homomorphic encryption. Concurrency and Computation: Practice and Experience, page e5817, 2020.
[8] Dalia Khader, Ben Smyth, Peter Ryan, and Feng Hao. A fair and robust voting system by broadcast. Lecture Notes in Informatics, pages 285– 299, 2012.
[9] K. Lee, J. James, T. Ejeta, and H. Kim. Electronic voting service using blockchain. Journal of Digital Forensics, Security and Law, 11, 2016. https://doi.org/10.15394/jdfsl.2016.1383.
[10] Patrick McCorry, Siamak F. Shahandashti, and Feng Hao. A smart contract for boardroom voting with maximum voter privacy. In Aggelos Kiayias, editor, Financial Cryptography and Data Security, pages 357– 375, Cham, 2017. Springer International Publishing.
[11] Stefano Bistarelli, Marco Mantilacci, Paolo Santancini, and Francesco Santini. An end-to-end voting system based on bitcoin. In Proceedings of the Symposium on Applied Computing, SAC '17, pages 1836– 1841, New York, NY, USA, 2017. ACM.
[12] Gongxian Zeng, Meiqi He, and Siu Ming Yiu. A secure and self-tallying e-voting system based on blockchain. In International Workshop on Information Security Applications, pages 67–76. Springer, 2019.

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com